Trust Anchors are Invulnerable

A Cyber Security Assumption Buster Workshop Series

Assertion: "Trust anchors are invulnerable"

Significant cyber security research and development is aimed at developing and implementing invulnerable trust anchors, security keystones that cannot be circumvented and that assure that trust in a system is well grounded. Much of this research is based on the following assumptions:

- Numerous trust anchors are proffered at different levels of assurance and for different aspects of the system.
- Platform trust is assured by the Trusted Platform Module.
- Trust authentication is provided by tokens.
- The padlock on the browser assures we can trust web interactions since they are protected by SSL.
- Close-held keys and strong key management systems assure cryptographic trust.

All of this research promises users who faithfully deploy reliable trust anchors that they can be confident that they are immune from the attacks for which the trust anchor provides protection.

In this workshop, we will explore whether, or in what circumstances, this confidence is warranted. We will challenge the notion that it is reasonable to assert absolute trust. We will consider what effect the introduction of the notion of a determined adversary has on our belief in trustworthiness. Through a series of sessions, we will examine several trust anchors, to include PKI, cryptographic tokens, the Trusted Platform Module, and the computing platform (operating system and hardware). During each session we will identify what assurances are provided by that trust anchor, explore how the trust anchor depends upon and interacts with the rest of the system, discuss how things go wrong even in systems that employ such anchors, and consider what is needed to enable the effective use of the anchor in a complete system.

Proposed Trust Anchors Questions:

How do trust anchors take into account the adversary's cost/benefit equation?
What are the residual risk reflections introduced by trust anchors?
In what contexts can we reasonably rely on trust anchors?
Can you layer trust anchors?
If you layer trust anchors is security increased?
How do layers of trust anchors interact with each other?
Are there unintended consequences to layer trust anchors?
How do we determine the minimum amount of mechanisms needed to support the trust anchor?
What constitutes a "safe" execution/storage environment for a trust anchor and how can it be created?
How do you monitor the status of a trust anchor?
What mechanisms can be put in place to know when trust anchors fail?
How do we design detection mechanisms that detect quicker than a successful attack?
How can trust anchors, once deployed, evolve over time?
For whom is the trust anchor providing trust?